Reuben D. Nathan, Esq. (SBN 208436)
NATHAN & ASSOCIATES, APC
2901 W. Coast Hwy., Suite 200
Newport Beach, CA 92663
Office: (949) 270-2798
Email: rnathan@nathanlawpractice.com

Ross Cornell, Esq. (SBN 210413)
LAW OFFICES OF ROSS CORNELL, APC
40729 Village Dr., Suite 8 - 1989
Big Bear Lake, CA 92315
Office: (562) 612-1708
Email: rc@rosscornelllaw.com

Attorneys for Plaintiff: TANYA ARNOLD

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

TANYA ARNOLD, on behalf of herself and all similarly situated persons,

Plaintiff,

v.

ROCKET COMPANIES, INC., a Delaware corporation,

Defendants.

Case No:

COMPLAINT

1. Cal. Penal Code § 638.51
2. Cal. Bus. & Prof. Code § 17200, *et seq.*

CLASS ACTION

I. NATURE OF THE ACTION

1. Defendant ROCKET COMPANIES, INC., a Delaware corporation, (referred to herein as "Defendant" or "ROCKET") owns and operates a website, www.rocketmortgage.com (the "Website").

2. This is a class action lawsuit brought by Plaintiff on behalf of herself and on behalf of all California residents who have accessed the Website.

3. Plaintiff TANYA ARNOLD files this class action complaint on behalf of herself and all others similarly situated (the "Class Members") against Defendant. Plaintiff brings this action based upon personal knowledge of the facts pertaining to her, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

4. A pixel tracker, also known as a web beacon, is a tracking mechanism embedded in a website that monitors user interactions. It typically appears as a small, transparent 1x1 image or a lightweight JavaScript snippet that activates when a webpage is loaded or a user performs a tracked action.

5. When triggered, the pixel transmits data from the user's browser to a third-party server. This data typically includes page views, session duration, referrer URLs, IP address, browser and device details, and other interaction metadata.

6. When users visit the Website, Defendant causes tracking technologies to be installed, executed, embedded, or injected in visitors' browsers. These include, but are not limited to, the following:

- Google Ads / DoubleClick Tracker
- Facebook PixelTracker
- Snapchat Tracker

7. The third parties who operate the above-listed trackers use pieces of User Information (defined below) collected via the Website as described herein for their own independent purposes tied to broader advertising ecosystems, profiling, and data

monetization strategies that go beyond Defendant's direct needs for their own financial gain. The above-listed trackers are referred to herein collectively as the "Trackers."

8. The Trackers are operated by distinct third parties: Google LLC (Google Ads / DoubleClick Tracker), Meta Platforms, Inc. (Facebook Pixel Tracker) and Snap Inc. (Snapchat Tracker). Defendant enables these trackers, which transmit user data to their respective third-party servers to identify users and support targeted advertising, user profiling, and data monetization within each platform's advertising ecosystem.

9. Through the Trackers, the Third Parties collect detailed user information including IP addresses, browser and device type, screen resolution, operating system, pages visited, session duration, mouse movements, click behavior**,** referring URLs, unique identifiers (such as cookies and ad IDs), and geolocation based on IP. This information is used for behavioral profiling, ad targeting, cross-device tracking, and participation in real-time advertising auctions (collectively, "User Information").

10. Because the Trackers capture and transmit users' IP addresses, full page URLs, referrer headers, device identifiers, and other non-content metadata, they function as "pen registers" and/or "trap and trace devices" under Cal. Penal Code § 638.50. These tools silently collect routing and addressing information for commercial use without user interaction, as defined in *Greenley v. Kochava, Inc*., 2023 WL 4833466 (S.D. Cal. July 27, 2023).

11. Plaintiff and the Class Members did not consent to the installation, execution, embedding, or injection of the Trackers on their devices and did not expect their behavioral data to be disclosed or monetized in this way. By installing and using the Trackers without prior consent and without a court order, Defendant violated CIPA section 638.51.

12. By installing and activating the Trackers without obtaining user consent or a valid court order, Defendant violated California Penal Code § 638.51, which prohibits the use of pen registers and trap and trace devices under these circumstances.

13. Defendant provides a privacy policy referred to as "Rocket Family of Companies Privacy Policy" (the "Privacy Policy") on the Website. On information and belief, Defendant, by and through the Website, does not conform to the Privacy Policy:

a. Defendant represents in its Privacy Policy that it engages third party companies and individuals to help operate, provide, and advertise its services, and states that such third parties are permitted to use personal information solely to perform services on Defendant's behalf. However, the Website transmits personal information including unique identifiers and browsing behavior to third party advertising and analytics companies immediately upon site access, without any apparent technical enforcement of purpose limitation or downstream use restrictions. This practice is inconsistent with Defendant's narrow framing of data use as being limited to discrete service provider functions;

b. Defendant does not clearly disclose that real-time behavioral data is transmitted to third parties immediately upon site arrival;

c. Defendant represents that the Website uses data analytics software to improve its services and that Defendant relies on consumer consent to personalize advertisements on third-party platforms. In reality, the Website provides no initial consent mechanism;

d. Tracking and third-party sharing occurs prior to presenting users with a valid choice to opt-out or manage consent; and

e. Defendant omits material details regarding the depth of personal data shared with third parties and the nature of behavioral profiling activities.

14. Plaintiff brings this action to prevent Defendant from further violating the privacy rights of California residents.

/ /

15. Generalized references herein to users, visitors and consumers expressly include Plaintiff and the Class Members.

II. PARTIES

16. Plaintiff TANYA ARNOLD ("Plaintiff") is a California citizen residing in Riverside County and has an intent to remain there. Plaintiff was in California when she visited the Website, which occurred during the class period prior to the filing of the complaint in this matter. The allegations set forth herein are based on the Website as configured when Plaintiff visited it.

17. Defendant ROCKET COMPANIES, INC. is a Delaware Corporation that owns, operates and/or controls the Website which is an online platform that offers goods and services to consumers.

18. ROCKET is one of the largest mortgage lending and financial technology platforms in the United States. Headquartered at 1050 Woodward Avenue, Detroit, Michigan, ROCKET operates its primary digital presence through the consumer-facing Website. The company provides consumers, real estate professionals, and financial partners with access to mortgage products, loan servicing tools, and digital solutions designed to streamline the financing and homeownership process. Through this platform, ROCKET facilitates key customer and partner interactions, showcases its suite of services, and enables secure access to account management portals and informational resources.

19. The Website serves as the flagship online platform for ROCKET and plays a central role in the company's digital operations. Beyond supporting loan origination and servicing, the website is responsible for processing user data linked to browsing activity, service inquiries, and account usage. As part of these business operations, ROCKET collects and processes substantial amounts of personally identifiable information and behavioral metadata. These data practices support lead generation, personalized digital experiences, and ongoing consumer communications.

/ /

III. JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because the total matter in controversy exceeds $5,000,000 and there are over 100 members of the proposed class. Further, at least one member of the proposed class is a citizen of a State within the United States and at least one defendant is the citizen or subject of a foreign state.

21. This Court has personal jurisdiction over Defendant because, on information and belief, Defendant has purposefully directed its activities to the Central District of California by regularly engaging with individuals in California through its website. Defendant's illegal conduct is directed at and harms California residents, including Plaintiff, and if not for Defendant's contact with the forum, Plaintiff would not have suffered harm.

22. Venue is proper in the Central District of California pursuant to 28 U.S.C. § 1391 because Defendant (1) is authorized to conduct business in this District and has intentionally availed itself of the laws and markets within this District; (2) does substantial business within this District; (3) is subject to personal jurisdiction in this District because it has availed itself of the laws and markets within this District; and (4) the injury to Plaintiff occurred within this District.

IV. GENERAL ALLEGATIONS

1. *The California Invasion of Privacy Act (CIPA)*

23. Enacted in 1967, the California Invasion of Privacy Act (CIPA) is a legislative measure designed to safeguard the privacy rights of California residents by prohibiting unauthorized wiretapping and eavesdropping on private communications. The California Legislature recognized the significant threat posed by emerging surveillance technologies, stating that "the development of new devices and techniques for the purpose of eavesdropping upon private communications … has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society" (Cal. Penal Code § 630).

24. CIPA specifically prohibits the installation or use of "pen registers" and "trap and trace devices" without consent or a court order (Cal. Penal Code § 638.51(a)).

25. A "pen register" is defined as a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, excluding the contents of the communication (Cal. Penal Code § 638.50(b)).

26. Conversely, a "trap and trace device" captures incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, again excluding the contents (Cal. Penal Code § 638.50(b)).

27. In practical terms, a pen register records outgoing dialing information, while a trap and trace device records incoming dialing information.

28. Historically, law enforcement has utilized these devices to monitor telephone calls, with pen registers recording outgoing numbers dialed from a specific line and trap and trace devices recording incoming call numbers to that line.

29. Although originally focused on landline telephone calls, CIPA's scope has expanded to encompass various forms of communication, including cell phones and online interactions. For instance, if a user sends an email, a pen register could record the sender's email address, the recipient's email address, and the subject line—essentially capturing the user's outgoing information.

30. Similarly, if the user receives an email, a trap and trace device could record the sender's email address, the recipient's email address, and the subject line—capturing the incoming information.

31. Despite predating the Internet, CIPA has been interpreted by the California Supreme Court to apply to new technologies where such application does not conflict with the statutory scheme (*In re Google Inc.*, 2013 WL 5423918, at *21; *Greenley*, supra, 2023 WL 4833466, at *15; *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1). This interpretation aligns with the principle that CIPA should be

construed to provide the greatest privacy protection when faced with multiple possible interpretations (*Matera v. Google Inc.*, 2016 WL 8200619, at *19).

32. The conduct alleged herein constitutes a violation of a legally protected privacy interest that is both concrete and particularized. Invasions of privacy have long been actionable under common law. (*Patel v. Facebook*, 932 F.3d 1264, 1272 (9th Cir. 2019); Eichenberger v. ESPN, Inc., 876 F.3d 979, 983 (9th Cir. 2017).)

33. Both the legislative history and statutory language indicate that the California Legislature intended CIPA to protect core privacy rights. Courts have found that violations of CIPA give rise to concrete injuries sufficient to confer standing under Article III. (See *Campbell v. Facebook, Inc.*, 2020 WL 1023350; *In re Facebook Internet Tracking Litig*., 956 F.3d 589 (9th Cir. 2020).)

34. Individuals may pursue legal action against violators of any CIPA provision, including Section 638.51, and are entitled to seek $5,000 in statutory penalties per violation (Cal. Penal Code § 637.2(a)(1)).

2. *The Trackers Are "Pen Registers" and/or "Trap and Trace Devices"*

35. When the Plaintiff and Class Members accessed the Website, their browsers initiated an HTTP or HTTPS request to Defendant's web server, which hosts the content and functionality of the site. In response, the server transmitted an HTTP response containing the necessary resources including HTML, cascading style sheets (CSS), JavaScript files, and image assets used by the browser to render and display the webpage. These resources also included client-side scripts that initiate communication with third-party services for analytics, marketing, and tracking purposes. ***Figure 1*** below illustrates sample HTTP requests.

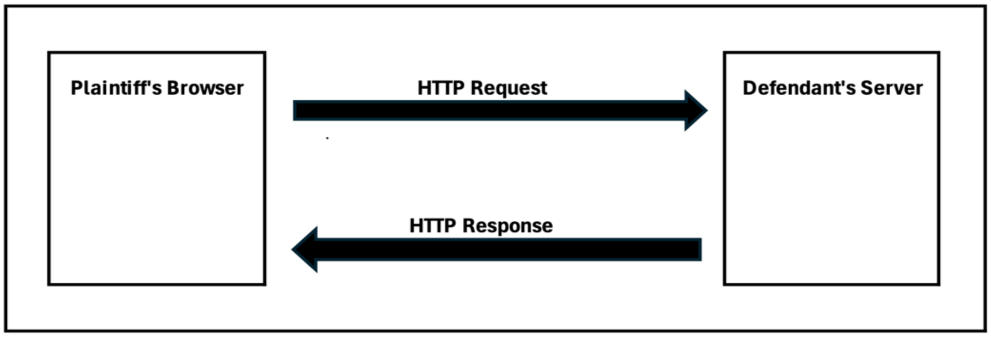
/ /

/ /

/ /

/ /

Figure 1



36. The server's response included third-party tracking scripts that were executed by the Plaintiff's and Class Members' web browsers. These scripts, once executed, initiate client-side functions that capture routing and behavioral metadata and transmit this data typically via HTTPS requests to the servers of third-party tracking vendors. These actions occur without visible indicators or user awareness. The transmitted data, referred to as User Information, included identifiers such as IP addresses, device characteristics, browser types, page navigation behavior, and unique tracking cookies, all of which were used to profile users and facilitate targeted advertising.

37. The Trackers operate by initiating HTTP or HTTPS requests—using either the GET or POST method from the user's browser to external servers controlled by the Third Parties. These requests are triggered automatically during the page load and by user interactions with the Website. They are used to transmit behavioral data and device metadata, including information such as page views, click events, session duration, and identifying browser characteristics.

38. An Internet Protocol (IP) address is a numerical identifier assigned to each device or network connected to the Internet, used to facilitate communication between systems. *See hiQ Labs, Inc. v. LinkedIn Corp.* (9th Cir. 2019) 938 F.3d 985, 991 n.4. The most common format, known as IPv4, consists of four numbers separated by periods (e.g., 191.145.132.123). IP addresses enable routing of data between devices

and can be used via external geolocation services to infer a user's general location, including state, city, and in some cases, ZIP code.

39. Public IP addresses are unique identifiers assigned by Internet Service Providers (ISPs) that allow devices to communicate directly over the Internet. They are globally accessible, meaning they can be reached from anywhere on the Internet, but are not inherently exposed unless data is being transmitted. Public IP addresses are essential for devices requiring direct Internet access and can be used to approximate a device's physical location through geolocation services.

40. In contrast, private IP addresses are used within internal networks and are not routable on the public Internet. They are isolated from the global Internet and can be reused across different networks without conflict. Unlike public IP addresses, private IP addresses do not divulge a user's geolocation.

41. Public IP addresses play a significant role in digital marketing by enabling geographic targeting based on a user's approximate location. Through IP geolocation services, advertisers can often determine a user's country, region, city, and in some cases, ZIP code or service area. In contexts where a static IP address is associated with a fixed residence or business, this data can contribute to household-level or business-level targeting, particularly when combined with other tracking identifiers and third-party enrichment.

42. A public IP address functions as "routing, addressing, or signaling information" by facilitating internet communication. It provides essential information that can help determine the general geographic coordinates of a user accessing a website through geolocation databases. Additionally, a public IP address is involved in routing communications from the user's router to the intended destination, ensuring that emails, websites, streaming content, and other data reach the user correctly.

43. As "routing, addressing, or signaling information," a public IP address is indispensable for maintaining seamless and efficient communication over the Internet.

It ensures that data packets are sent from the user's router to the intended destination, such as a website or email server.

44. Defendant installs Trackers on users' browsers to collect User Information, including IP addresses and full URLs, which constitute outgoing routing and addressing metadata under CIPA. These identifiers serve the same function as telephony dialed numbers and therefore meet the statutory definition of a pen register or trap and trace device.

3. *The Use of Pixel Trackers or Beacons and Digital Fingerprinting*

45. Website users typically expect a degree of anonymity when browsing, particularly when they are not logged into an account. However, upon visiting the Website, Plaintiff's and Class Members' browsers executed third-party tracking scripts embedded by the Defendant. These Trackers operate in the background of the browsing session and collect detailed behavioral and technical information, which is then transmitted to external third-party servers without the users' active awareness.

46. This process, known as digital fingerprinting, involves compiling various data points such as browser version, screen resolution, installed fonts, device type, and language settings to generate a unique identifier for each user. Fingerprinting can be used to recognize repeat visits and correlate activity across different sessions or sites. When combined with form inputs, login activity, or third-party enrichment, fingerprinting can contribute to broader profiling of a user's interests, affiliations, or behaviors.

47. When combined with additional tracking mechanisms such as cookies, login data, and third-party enrichment services, fingerprinting contributes to user profiling. This may include inferring location, browsing habits, consumer preferences, and potentially associating these patterns with known user identities. A sufficiently detailed digital fingerprint, especially when correlated with other identifiers such as email addresses, form submissions, or third-party databases, can enable the reidentification of a user.

48. The ability to associate a persistent digital profile with a specific individual using techniques such as digital fingerprinting has led to the development of a data industry known as identity resolution. Identity resolution involves recognizing users across sessions, devices, and platforms by connecting various identifiers derived from their digital behavior, including IP addresses, browser metadata, cookies, and, in some cases, login credentials. The process may occur deterministically (based on known logins or user-submitted information) or probabilistically (based on behavioral or technical similarity).

49. In simpler terms, pen register and trap and trace mechanisms in the digital context refer to technologies that record metadata such as IP addresses, URLs visited, and device characteristics, information that identifies the routing and addressing of electronic communications. This can be achieved through the deployment of tracking technologies like the Trackers installed, executed, embedded or injected in the Website, which operate without user interaction or visibility.

50. The Trackers provide analytics and marketing services to Defendant using the data collected from visitors to the Website. These services also leverage user data collected from other websites that include the same pen register and trap and trace devices operated by the Third Parties.

51. When users visit the Website, installed, executed, embedded or injected Trackers initiate network requests to third-party servers, using invisible image pixels, JavaScript calls, or beacon APIs. These requests include the user's IP address, which is transmitted automatically as part of the HTTP request header. In many cases, the Tracker's server responds by placing a persistent cookie in the user's browser, which serves as a unique identifier that can be used to recognize and track the user across future visits. If a user deletes their browser cookies, this identifier is removed. However, upon revisiting the Website, the process repeats: the browser executes the Tracker's script, a new identifier is set, and the Tracker resumes collecting the user's IP address and associated behavioral data.

4. *Plaintiff's And Class Members' Data Has Financial Value*

52. Given the number of Internet users, the "world's most valuable resource is no longer oil, but data."[1]

53. Consumers' web browsing histories have an economic value more than $52 per year, while their contact information is worth at least $4.20 per year, and their demographic information is worth at least $3.00 per year.[2]

54. There is "a study that values users' browsing histories at $52 per year, as well as research panels that pay participants for access to their browsing histories."[3]

55. Extracted personal data can be used to design products, platforms, and marketing techniques. A study by the McKinsey global consultancy concluded that businesses that "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[4]

56. In 2013, the Organization for Economic Cooperation and Development ("OECD") estimated that data trafficking markets had begun pricing personal data, including those obtained in illicit ways without personal consent. It found that illegal markets in personal data valued each credit cardholder record at between 1 and 30 U.S. dollars in 2009, while bank account records were valued at up to 850 U.S. dollars. Data brokers sell customer profiles of the sort that an online retailer might collect and

[1] Ian Cohen, Are Web-Tracking Tools Putting Your Company at Risk?, Forbes (Oct 19, 2022), https://www.forbes.com/sites/forbestechcouncil/2022/10/19/are-web-tracking-tools-putting-your-company-atrisk/?sh=26481de07444

[2] *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 928 (N.D. Cal. 2015), rev'd, 956 F.3rd 589 (9th Cir. 2020).

[3] *In re Facebook, Inc. Internet Tracking Litigation* (9th Cir. 2020) 956 F.3rd 589, 600.

[4] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, Capturing value from your customer data, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/businessfunctions/quantumblack/ourinsights/capturing-value-from-your-customer-data

maintain for about 55 U.S. dollars, and that individual points of personal data ranged in price from $0.50 cents for an address, $2 for a birthday, $8 for a social security number, $3 for a driver's license number, and $35 for a military record (which includes a birth date, an identification number, a career assignment, height, weight, and other information). Experiments asking individuals in the United States and elsewhere how much they value their personal data points result in estimates of up to $6 for purchasing activity, and $150-240 per credit card number or social security number.[5]

57. The last estimate probably reflects public reporting that identify theft affecting a credit card number or social security number can result in financial losses of up to $10,200 per victim.[6]

58. The Defendant's monetization of personal data constitutes actionable economic harm under federal law, even without evidence of a direct financial loss, as a "misappropriation-like injury" caused by converting user data into a revenue stream through targeted advertising. *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020).

5. *Defendant Is Motivated To Monetize Consumer Information Regardless of Consent*

59. Data harvesting is one of the fastest growing industries in the country, with estimates suggesting that internet companies earned $202 per American user in 2018 from mining and selling data. That figure is expected to increase with estimates for 2022 as high as $434 per use, reflecting a more than $200 billion industry.

60. By implementing Trackers on the Website, Defendant participates in building detailed behavioral profiles of visitors. These profiles may include information

[5] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, No. 220 (Apr. 2, 2013), at 27-28, https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf

[6] Bradley J. Fikes, Identity Theft Hits Millions, Report Says, San Diego Union Tribune, Sept. 4, 2003, https://www.sandiegouniontribune.com/sdut-identity-theft-hits-millions-report-says-2003sep04-story.html.

such as which users viewed specific products, engaged with pages or interface elements, or demonstrated purchase intent. This data enables Defendant and its advertising partners to identify repeat visits from the same device or browser. The behavioral data is integrated into third-party advertising platforms, allowing Defendant to deliver retargeted ads to users who previously visited the Website, offer promotional incentives to re-engage high-intent visitors, and build "lookalike audiences" that target users with similar behaviors or characteristics. These practices significantly improve advertising efficiency and increase the likelihood of converting user engagement into actual sales.

61. Defendant has a strong financial incentive to deploy the Trackers on its Website without obtaining user consent. By enabling the collection of IP addresses and device-level identifiers through these technologies, Defendant facilitates integration into real-time bidding ecosystems. These systems rely on bidstream data such as IP address, device type, screen resolution, and referral information to assess the value of a potential ad impression. This enables Defendant and its partners to participate in data-driven ad targeting, increase the value of its advertising inventory, and track users across sessions and websites, all of which provide economic benefit despite private implications to users.

62. IP addresses are a valuable data point in digital advertising and tracking systems. They can be used to approximate a user's geographic location, often down to the city or ZIP code level, enabling location-based targeting. When combined with cookies, browser metadata, and device identifiers, IP addresses contribute to persistent user tracking across sessions and websites. They also assist advertisers and data brokers in linking anonymous browsing activity to existing user profiles, which enhances ad targeting precision and increases the commercial value of each tracked interaction. IP addresses therefore constitute "routing, addressing, or signaling information" protected under CIPA § 638.50(b).

63. When users' data is collected without meaningful consent and monetized, they lose control over who can access, use, or distribute their personal information. Data

brokers and ad tech firms aggregate and correlate identifiers such as IP addresses, device IDs, and cookies with other personal data to construct detailed consumer profiles. Information initially gathered in one context, such as browsing a retail website, is frequently repurposed for unrelated uses and sold to third parties without the user's awareness. This results in pervasive surveillance, where users are continuously tracked across multiple websites, applications, and devices, often without their knowledge or ability to opt out.

6. ***The Trackers Function Together to Achieve Targeted Objectives***

64. When a user visits the Website, a suite of background tracking technologies is silently activated upon initial page load. These include client side scripts (Trackers) deployed by Google Ads and DoubleClick, Facebook Pixel and SnapChat Pixel, all of which begin collecting user information immediately and without visible notice. These technologies work together to form a coordinated data collection infrastructure that allows ROCKET and its marketing partners to observe user behavior in real time. The information collected is used to optimize marketing campaigns, segment audiences, and enhance targeting precision for digital advertising initiatives.

65. On information and belief, these third party trackers operate as part of a large scale, interconnected digital advertising ecosystem. Entities such as Google, Meta (Facebook) and Snapchat utilize shared identifiers, cookie syncing, and cross device recognition technologies to follow users across disparate websites, devices, and platforms. These tools are specifically designed to enable persistent identity resolution and real time behavioral targeting, facilitating the construction of detailed consumer profiles at scale.

66. On the Website, these trackers are embedded either directly in the site's HTML source or are dynamically loaded via JavaScript during runtime. Google Ads and DoubleClick and the Facebook Pixel are triggered immediately upon landing on the homepage. Simultaneously, tracking requests from SnapChat's Pixel, which are also initiated with no gating or opt in mechanism. These technologies collect a variety of

data points including IP address, device configuration, browser characteristics, and on site interactions and transmit them to third party servers. Their joint purpose is to enable downstream advertising activities, identity correlation, and behavior based audience monetization.

67. Identity resolution on the Website is primarily enabled through the interplay of Facebook and SnapChat tracking tools. The Facebook Pixel associates website activity with logged in Facebook user sessions and stored cookies, allowing Meta to build cross context behavioral profiles. SnapChat's tracking endpoint captures user engagement and potentially device level attributes to enable lookalike modeling and campaign retargeting. These integrated mechanisms enable ROCKET and its partners to de anonymize site visitors over time and associate browsing behavior with real world identities and demographic attributes.

68. Once identity signals are collected, targeted advertising and audience segmentation are executed via platforms such as Google Ads and DoubleClick. Google's ad stack engages in real time programmatic auctions, delivering personalized ad creatives based on inferred intent, user demographics, and conversion signals. The SnapChat Pixel contributes to dynamic audience building and conversion tracking across devices. Together, these systems allow ROCKET and its advertising partners to monetize visitor behavior, optimize campaign performance, and deliver highly specific ad content across channels.

69. ROCKET shares user information with third party advertising platforms, particularly DoubleClick (a division of Google), that operate real time bidding systems. Upon visiting the website, data such as the user's IP address, browser type, page URL, and device details are transmitted to Google's ad infrastructure without any affirmative user action. These identifiers allow advertisers to follow users across the web, profile their behavior, and serve personalized ads in real time. Critically, this data exchange occurs immediately, without consent, and before the user can review or manage privacy preferences.

70. Network requests captured in the HAR file to DoubleClick's tracking endpoints confirm that ROCKET is participating in a programmatic advertising infrastructure that supports real time ad bidding and conversion tracking. These data transfers enable advertisers to compete for ad impressions based on a user's digital footprint, increasing the value of each visitor to the Website. Importantly, these requests serve no functional benefit to the user. They exist solely to enable ROCKET and its partners to extract commercial value from personal data. The silent activation of these trackers at page load transforms sensitive user information into a marketable asset for advertising return.

V. <u>SPECIFIC ALLEGATIONS</u>

1. Google Ads / DoubleClick Tracker

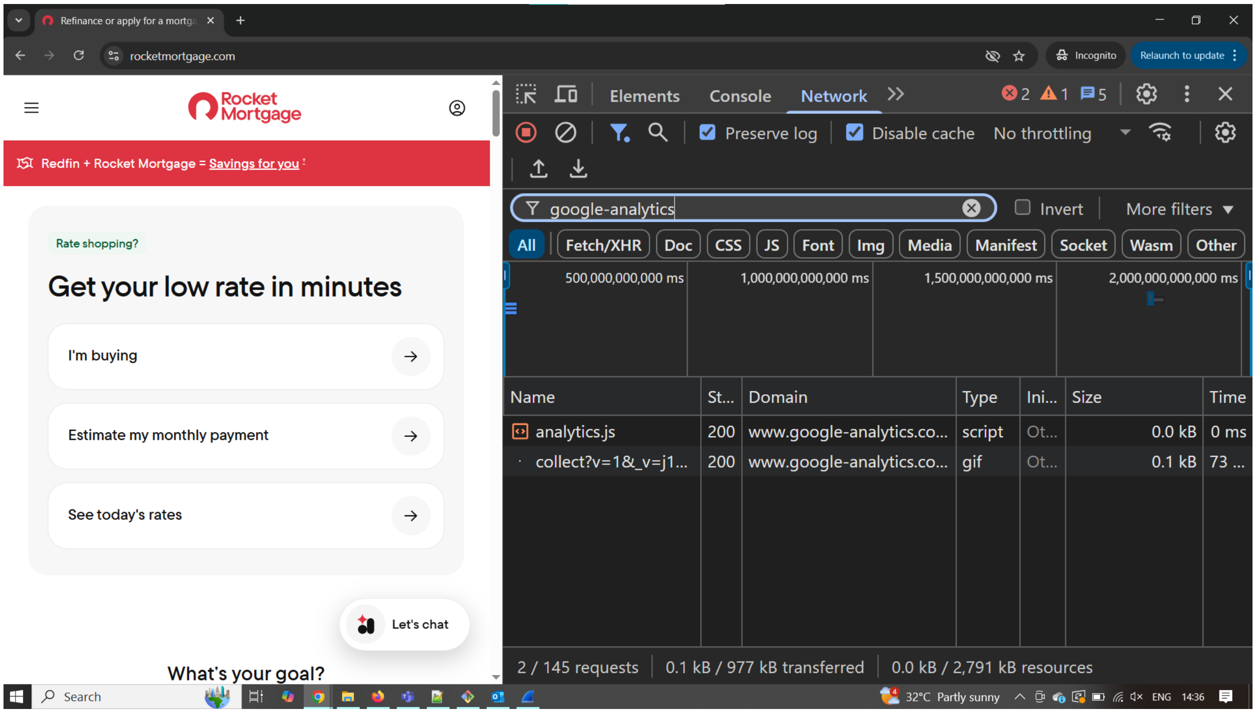
71. The Google Ads / DoubleClick Tracker is a digital advertising, behavioral tracking, and data brokering technology operated by Google LLC. It is designed to deliver display advertisements, measure engagement, and support real-time bidding on programmatic ad exchanges. The Google Ads / DoubleClick Tracker enables Google and its advertising clients to collect detailed user interaction data and optimize ad delivery across a vast network of third-party websites.

72. When implemented on the Website, the Google Ads / DoubleClick Tracker collects a broad set of user metadata, including visited URLs, session timestamps, referrer headers, and in-page activity data such as page views and navigation events. It also captures technical device attributes such as IP address, screen resolution, browser type, operating system, and language settings. These data points are linked to persistent browser identifiers placed via cookies or pixel fires that allow Google to track users across multiple websites, sessions, and devices, forming longitudinal behavioral profiles. The Google Ads / DoubleClick Tracker also transmits conversion tracking signals and remarketing data, enabling Google to associate Website interactions with ad conversion events and to retarget users across its advertising ecosystem.

73. The Google Ads / DoubleClick Tracker facilitates monitoring of user activity on the Website, including the capture of pageview events and other engagement signals that can be used to track user progression through various transactional flows. These interaction signals are transmitted to Google's ad infrastructure to facilitate targeted advertising, audience retargeting, and conversion tracking. The Google Ads / DoubleClick Tracker executes via JavaScript calls to domains including googleads.g.doubleclick.net and activates automatically upon page load without requiring any action by the user.

74. The following figures [***Figure 2***, ***Figure 3*** and ***Figure 4***] provide technical evidence of the Google Ads / DoubleClick Tracker being automatically activated during a user's visit to the Website. Each screenshot evidences network activity triggered by scripts embedded in the page source, resulting in HTTP or DNS requests to external tracking domains. These network events occurred without any user interaction, confirming that the tracking technologies were operating silently in the background.

Figure 2



☑ Preserve log ☑ Disable cache No throttling

google-analytics ☐ Invert More filters

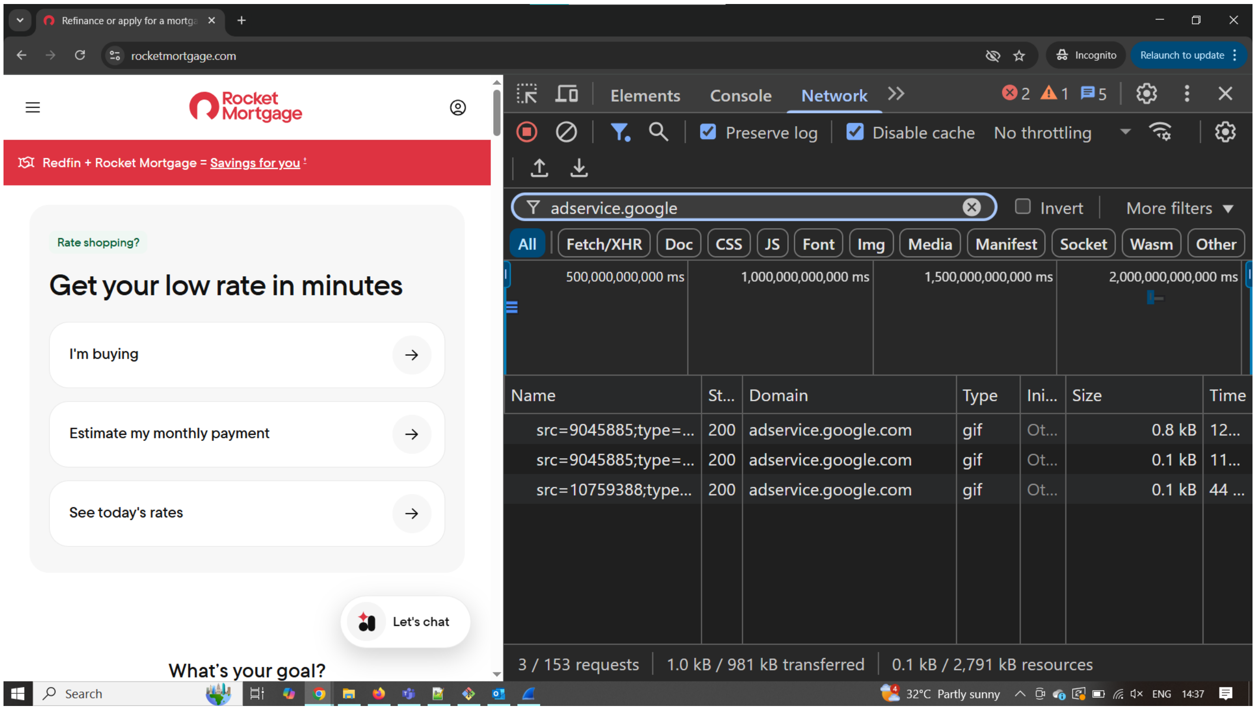
All | Fetch/XHR | Doc | CSS | JS | Font | Img | Media | Manifest | Socket | Wasm | Other

500,000,000,000 ms 1,000,000,000,000 ms 1,500,000,000,000 ms 2,000,000,000,000 ms

Name	St...	Domain	Type	Ini...	Size	Time
analytics.js	200	www.google-analytics.co...	script	Ot...	0.0 kB	0 ms
collect?v=1&_v=j1...	200	www.google-analytics.co...	gif	Ot...	0.1 kB	73 ...

2 / 145 requests | 0.1 kB / 977 kB transferred | 0.0 kB / 2,791 kB resources

Figure 3



Refinance or apply for a mortg

rocketmortgage.com

Rocket Mortgage

Redfin + Rocket Mortgage = Savings for you ¹

Rate shopping?

Get your low rate in minutes

I'm buying

Estimate my monthly payment

See today's rates

Let's chat

What's your goal?

Elements Console Network

☑ Preserve log ☑ Disable cache No throttling

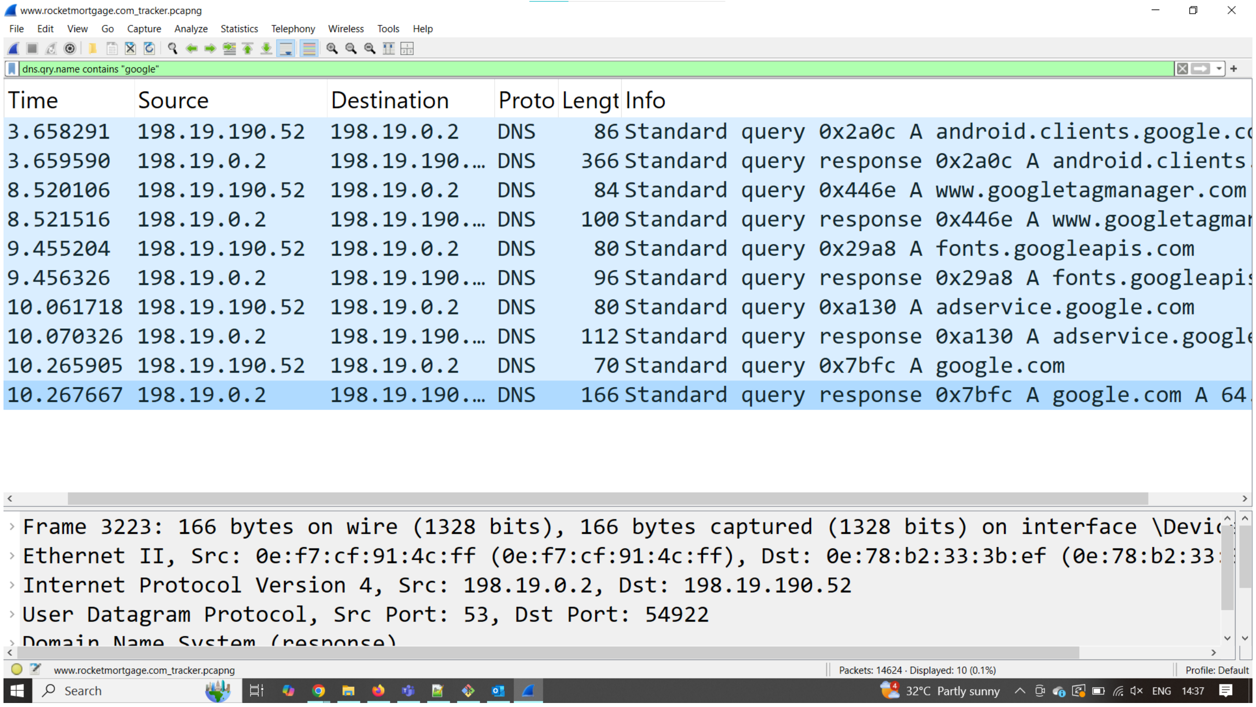
adservice.google □ Invert More filters

All Fetch/XHR Doc CSS JS Font Img Media Manifest Socket Wasm Other

Name	St...	Domain	Type	Ini...	Size	Time
src=9045885;type=...	200	adservice.google.com	gif	Ot...	0.8 kB	12...
src=9045885;type=...	200	adservice.google.com	gif	Ot...	0.1 kB	11...
src=10759388;type...	200	adservice.google.com	gif	Ot...	0.1 kB	44 ...

3 / 153 requests | 1.0 kB / 981 kB transferred | 0.1 kB / 2,791 kB resources

Figure 4



www.rocketmortgage.com_tracker.pcapng

dns.qry.name contains "google"

```
Time       Source         Destination    Proto Lengt Info
3.658291   198.19.190.52  198.19.0.2     DNS     86 Standard query 0x2a0c A android.clients.google.c
3.659590   198.19.0.2     198.19.190.... DNS    366 Standard query response 0x2a0c A android.clients
8.520106   198.19.190.52  198.19.0.2     DNS     84 Standard query 0x446e A www.googletagmanager.com
8.521516   198.19.0.2     198.19.190.... DNS    100 Standard query response 0x446e A www.googletagmar
9.455204   198.19.190.52  198.19.0.2     DNS     80 Standard query 0x29a8 A fonts.googleapis.com
9.456326   198.19.0.2     198.19.190.... DNS     96 Standard query response 0x29a8 A fonts.googleapis
10.061718  198.19.190.52  198.19.0.2     DNS     80 Standard query 0xa130 A adservice.google.com
10.070326  198.19.0.2     198.19.190.... DNS    112 Standard query response 0xa130 A adservice.google
10.265905  198.19.190.52  198.19.0.2     DNS     70 Standard query 0x7bfc A google.com
10.267667  198.19.0.2     198.19.190.... DNS    166 Standard query response 0x7bfc A google.com A 64
```

```
› Frame 3223: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) on interface \Devi
› Ethernet II, Src: 0e:f7:cf:91:4c:ff (0e:f7:cf:91:4c:ff), Dst: 0e:78:b2:33:3b:ef (0e:78:b2:33
› Internet Protocol Version 4, Src: 198.19.0.2, Dst: 198.19.190.52
› User Datagram Protocol, Src Port: 53, Dst Port: 54922
› Domain Name System (response)
```

Packets: 14624 · Displayed: 10 (0.1%) | Profile: Default

75. Defendant surreptitiously installed, executed, embedded or injected the Google Ads / DoubleClick Tracker onto users' browsers by embedding tracking scripts

in the Website's page source and by dynamically injecting additional JavaScript tracking code during runtime. When a user visits the Website, their browser automatically executes this code, which initiates outbound network requests to Google's advertising servers and transmits metadata including IP address, page URL, referrer information, device details, behavioral identifiers, and conversion tracking parameters as part of a third-party ad targeting, profiling, and data brokering system.

76. The Google Ads / DoubleClick Tracker is at least a "process" because it is software that identifies consumers, gathers data, and correlates that data.

77. The Google Ads / DoubleClick Tracker is at least a "device" because in order for software to work, it must be run on some kind of computing device. *See*, e.g., *James v. Walt Disney Co.* 2023 WL 7392285 at *13 (N.D. Cal. Nov. 8, 2023).

78. The Google Ads / DoubleClick Tracker functions as a pen register and/or trap and trace device under the California Invasion of Privacy Act because it captures outgoing signaling data such as URLs visited, timestamps, and referrer headers and also processes incoming metadata such as ad impressions and cookie-based session identifiers. These transmissions occur automatically during page load and without user participation, enabling Google to continuously log user behavior and associate it with broader advertising profiles.

79. Defendant never obtained a court order permitting the installation of a pen register or trap and trace device or process and did not obtain Plaintiff's or the Class Members' express or implied consent to install the Google Ads / DoubleClick Tracker on Plaintiff's and Class Members' browser or to collect or share data with Google.

80. Consequently, the Google Ads / DoubleClick Tracker violates CIPA regarding unauthorized use of a pen register and/or trap and trace device without prior consent or court order.

2. The Facebook Pixel Tracker

81. The Facebook Pixel Tracker is a behavioral tracking script implemented through Meta's Pixel technology, typically delivered via domains such as

connect.facebook.net and facebook.com/tr/. On the Website, the Facebook Pixel Tracker is injected through tag management infrastructure. Once loaded, it initiates background communication with Meta's servers and enables real-time tracking of user activity.

82. On the Website's homepage, the Facebook Pixel Tracker activates automatically upon page load and begins capturing behavioral data in real time. It records interaction signals such as page views and other engagement events without requiring any user action. The Facebook Pixel Tracker actively detects and collects additional user interaction, including click-based events and scrolling behavior. These signals are transmitted to Meta's servers and associated with the user's Facebook or Instagram profile, even if the user never directly interacts with any Meta service while on the Website.

83. The data collected by the Facebook Pixel Tracker supports identity resolution by linking behavioral data from the Website with individual user profiles across Meta's platforms. If the user is logged into Facebook, Instagram, or Messenger on the same device or browser, the Facebook Pixel Tracker can tie Website behavior to the user's unique Meta ID. Even if not logged in, Meta can assign a persistent identifier using cookies, browser fingerprinting, or pixel fire data. This enables the creation of robust cross-site behavioral profiles based on a user's activity on the Website.

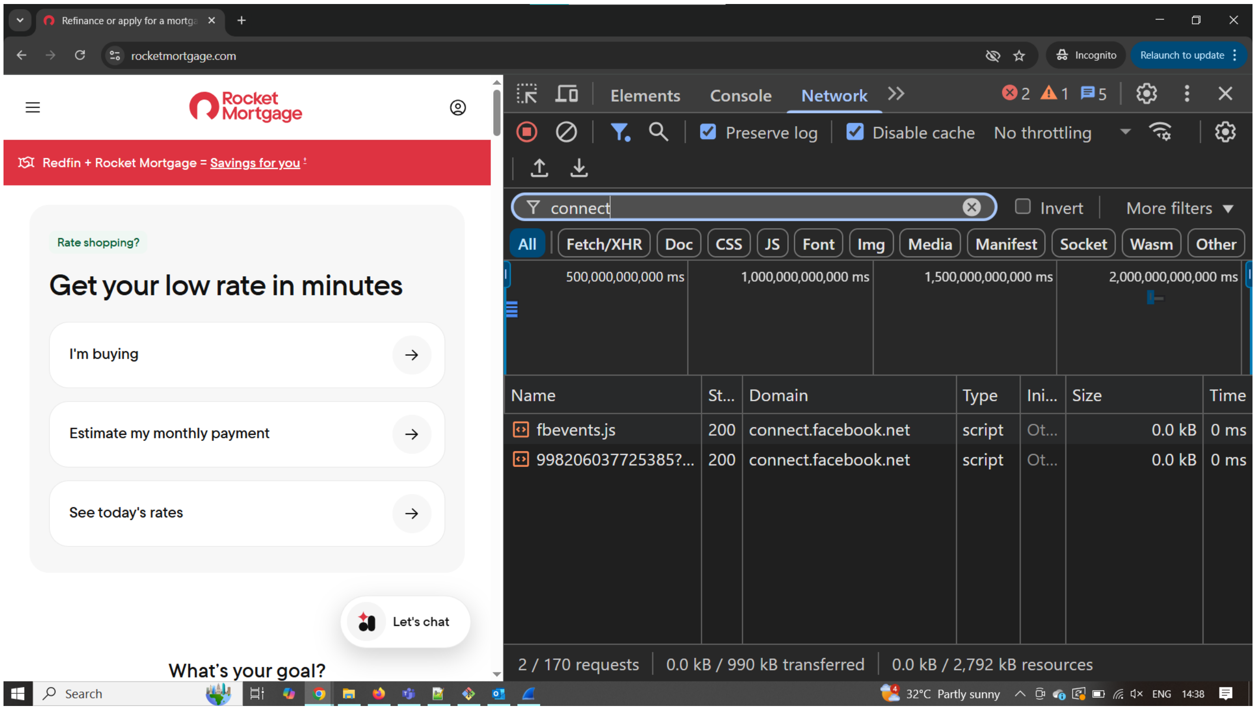
84. The Facebook Pixel Tracker also serves Defendant's goal of targeted advertising by enabling the creation of "Custom Audiences," groups of users who have taken specific actions on the Website, such as browsing listings, viewing product pages, or beginning a checkout process. ROCKET can then use Meta's Ads Manager to re-target those users across Facebook and Instagram, or to generate "Lookalike Audiences" that mirror the behavioral patterns of existing visitors. These mechanisms allow ROCKET to efficiently deliver marketing content to users most likely to engage or convert.

/ /

85. The Facebook Pixel Tracker contributes to ROCKET's data monetization strategy by turning behavioral insights into measurable advertising ROI. The Facebook Pixel Tracker generates real-time analytics regarding user behavior, campaign performance, and conversion attribution, which Meta then delivers to ROCKET through its Ads infrastructure. This closed-loop feedback system connects on-site engagement with off-site ad delivery, allowing ROCKET to refine ad spend, personalize messaging, and increase the value of each user interaction. In this way, the Facebook Pixel Tracker functions as a core part of ROCKET's commercial surveillance infrastructure.

86. The following figures [***Figure 5*** and ***Figure 6***] provide technical evidence of the Facebook Tracker being automatically activated during a user's visit to the Website. Each screenshot evidences network activity triggered by scripts embedded in the page source, resulting in HTTP or DNS requests to external tracking domains. These network events occurred without any user interaction, confirming that the tracking technologies were operating silently in the background.

Figure 5



rocketmortgage.com

Redfin + Rocket Mortgage = Savings for you

Rate shopping?

Get your low rate in minutes

I'm buying

Estimate my monthly payment

See today's rates

What's your goal?

☑ Preserve log ☑ Disable cache No throttling

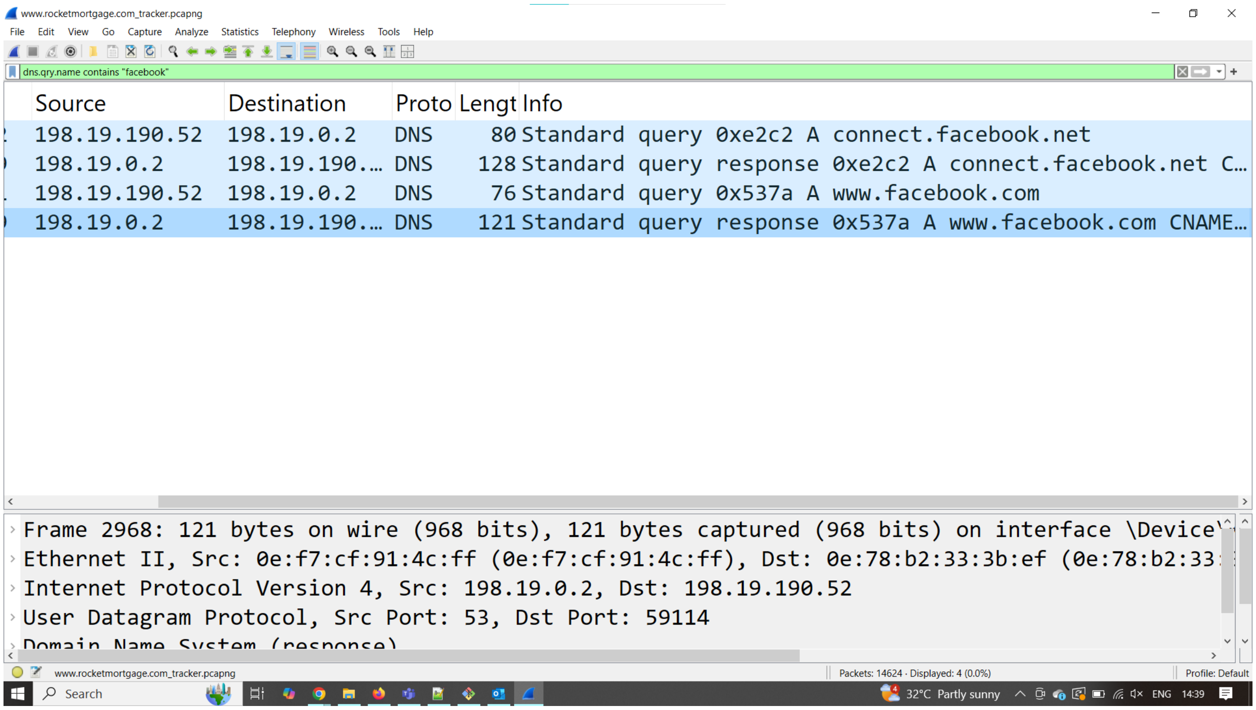
Filter: connect

□ Invert

Name	St...	Domain	Type	Ini...	Size	Time
fbevents.js	200	connect.facebook.net	script	Ot...	0.0 kB	0 ms
998206037725385?...	200	connect.facebook.net	script	Ot...	0.0 kB	0 ms

2 / 170 requests | 0.0 kB / 990 kB transferred | 0.0 kB / 2,792 kB resources

Figure 6


www.rocketmortgage.com_tracker.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns.qry.name contains "facebook"

```
Source          Destination     Proto Lengt Info
198.19.190.52   198.19.0.2      DNS     80 Standard query 0xe2c2 A connect.facebook.net
198.19.0.2      198.19.190.…    DNS    128 Standard query response 0xe2c2 A connect.facebook.net C…
198.19.190.52   198.19.0.2      DNS     76 Standard query 0x537a A www.facebook.com
198.19.0.2      198.19.190.…    DNS    121 Standard query response 0x537a A www.facebook.com CNAME…
```

```
> Frame 2968: 121 bytes on wire (968 bits), 121 bytes captured (968 bits) on interface \Device\
> Ethernet II, Src: 0e:f7:cf:91:4c:ff (0e:f7:cf:91:4c:ff), Dst: 0e:78:b2:33:3b:ef (0e:78:b2:33:
> Internet Protocol Version 4, Src: 198.19.0.2, Dst: 198.19.190.52
> User Datagram Protocol, Src Port: 53, Dst Port: 59114
> Domain Name System (response)
```

www.rocketmortgage.com_tracker.pcapng
Packets: 14624 · Displayed: 4 (0.0%)
Profile: Default
Search
32°C Partly sunny
ENG
14:39

87. Defendant surreptitiously installed, executed, embedded, or injected the Facebook Pixel Tracker onto users' browsers by dynamically injecting Meta's JavaScript pixel through a tag management system such as Google Tag Manager. When a user visits the Website, the browser automatically executes this script, triggering outbound requests to Meta's servers and transmitting metadata including the user's page URL, referrer, browser configuration, and other session-specific details. These tracking operations occur without any user interaction, allowing Meta to collect data from users' sessions silently and without their consent.

88. The Facebook Pixel Tracker is at least a "process" because it is software that identifies consumers, gathers data, and correlates that data.

89. The Facebook Pixel Tracker is at least a "device" because in order for software to work, it must be run on some kind of computing device. See, e.g., *James v. Walt Disney Co.* 2023 WL 7392285 at *13 (N.D. Cal. Nov. 8, 2023).

90. The Facebook Pixel Tracker captures and transmits routing, addressing, and signaling information such as the user's page URL, referrer, and browser metadata

to Meta's servers as soon as the page loads, without the user's knowledge or consent. This type of metadata reveals the origin and destination of the user's electronic communications. The connection is not initiated by the user, but rather by code embedded in the Website, allowing Meta to intercept and associate those signals with a known or inferred identity. The transmission occurs while the user's communication is still in transit and is diverted to Meta without authorization.

91. Defendant never obtained a court order permitting the installation of a pen register or trap and trace device or process and did not obtain Plaintiff's or the Class Members' express or implied consent to install the Facebook Pixel Tracker on Plaintiff's and Class Members' browser or to collect or share data with Facebook.

92. Consequently, the Facebook Pixel Tracker violates CIPA regarding unauthorized use of a pen register and/or trap and trace device without prior consent or court order.

3. The Snapchat Tracker

93. The Snapchat Tracker is a piece of software code that Defendant placed on the Website to share user interaction data and various Website events with Snapchat. This tracker enables the transmission of behavioral signals and technical metadata to Snapchat's tracking infrastructure, permitting Snapchat to monitor activity on the Website in real time and support the measurement and optimization of digital advertising campaigns.

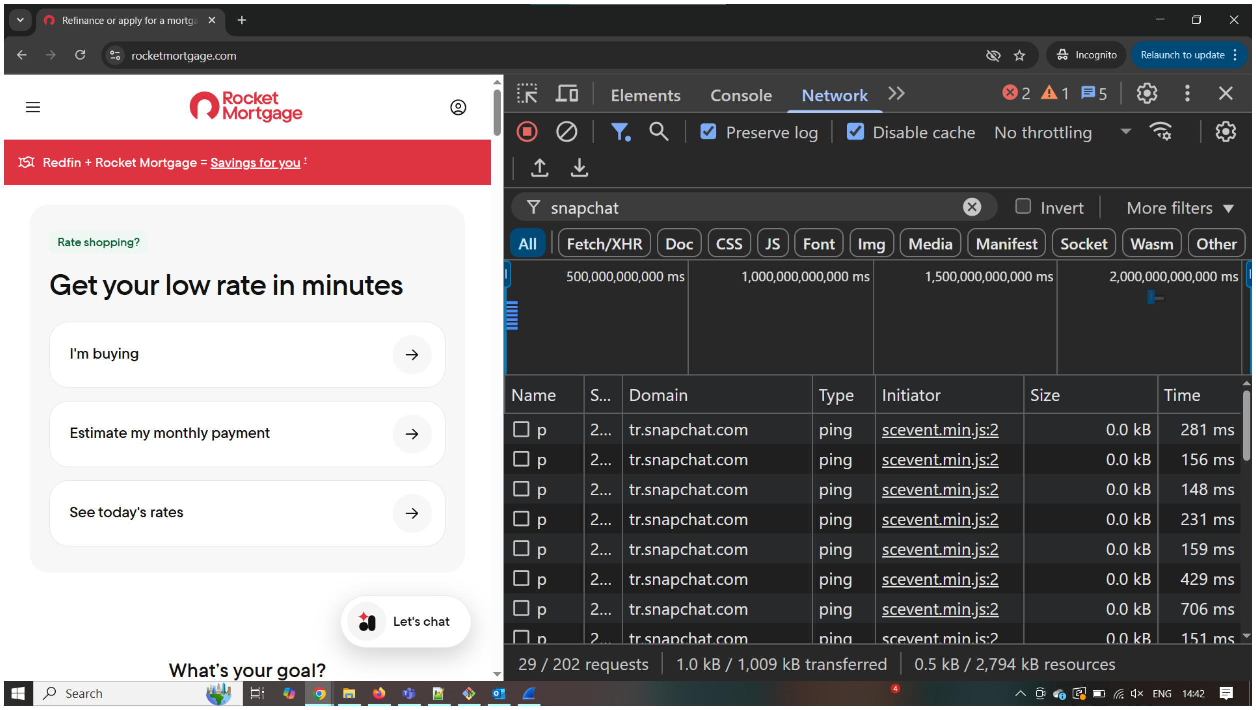
94. The Snapchat Tracker uses pixel-based surveillance mechanisms to collect and process user data on the Website as interactions occur. It monitors a range of events, including page views, button clicks, form submissions, and other engagement with site elements. This data is leveraged to analyze advertising effectiveness, facilitate behavioral targeting, and drive revenue by capturing and transmitting user information, including that of Plaintiffs and Class Members, to Snapchat's tracking systems.

95. The Snapchat Tracker begins collecting information immediately upon a user's arrival, gathering device and browser metadata, IP-based geolocation, HTTP

referrer headers, and the URL of the page visited together with other User Information. This information is sent to Snapchat in real time using JavaScript-based tracking scripts. Snapchat's tracking technologies acknowledge the automatic collection of User Information, transmitting that information to Snapchat's servers without requiring any affirmative user action.

96. The following figures [***Figure** 7* and ***Figure** 8*] provide technical evidence of Snapchat Tracker being automatically activated during a user's visit to the Website. Each screenshot evidences network activity triggered by scripts embedded in the page source, resulting in HTTP or DNS requests to external tracking domains. These network events occurred without any user interaction, confirming that the tracking technologies were operating silently in the background.

Figure 7



☑ Preserve log ☑ Disable cache No throttling

snapchat □ Invert More filters

All | Fetch/XHR | Doc | CSS | JS | Font | Img | Media | Manifest | Socket | Wasm | Other

500,000,000,000 ms 1,000,000,000,000 ms 1,500,000,000,000 ms 2,000,000,000,000 ms

Name	S...	Domain	Type	Initiator	Size	Time
□ p	2...	tr.snapchat.com	ping	scevent.min.js:2	0.0 kB	281 ms
□ p	2...	tr.snapchat.com	ping	scevent.min.js:2	0.0 kB	156 ms
□ p	2...	tr.snapchat.com	ping	scevent.min.js:2	0.0 kB	148 ms
□ p	2...	tr.snapchat.com	ping	scevent.min.js:2	0.0 kB	231 ms
□ p	2...	tr.snapchat.com	ping	scevent.min.js:2	0.0 kB	159 ms
□ p	2...	tr.snapchat.com	ping	scevent.min.js:2	0.0 kB	429 ms
□ p	2...	tr.snapchat.com	ping	scevent.min.js:2	0.0 kB	706 ms
□ p	2...	tr.snapchat.com	ping	scevent.min.js:2	0.0 kB	151 ms

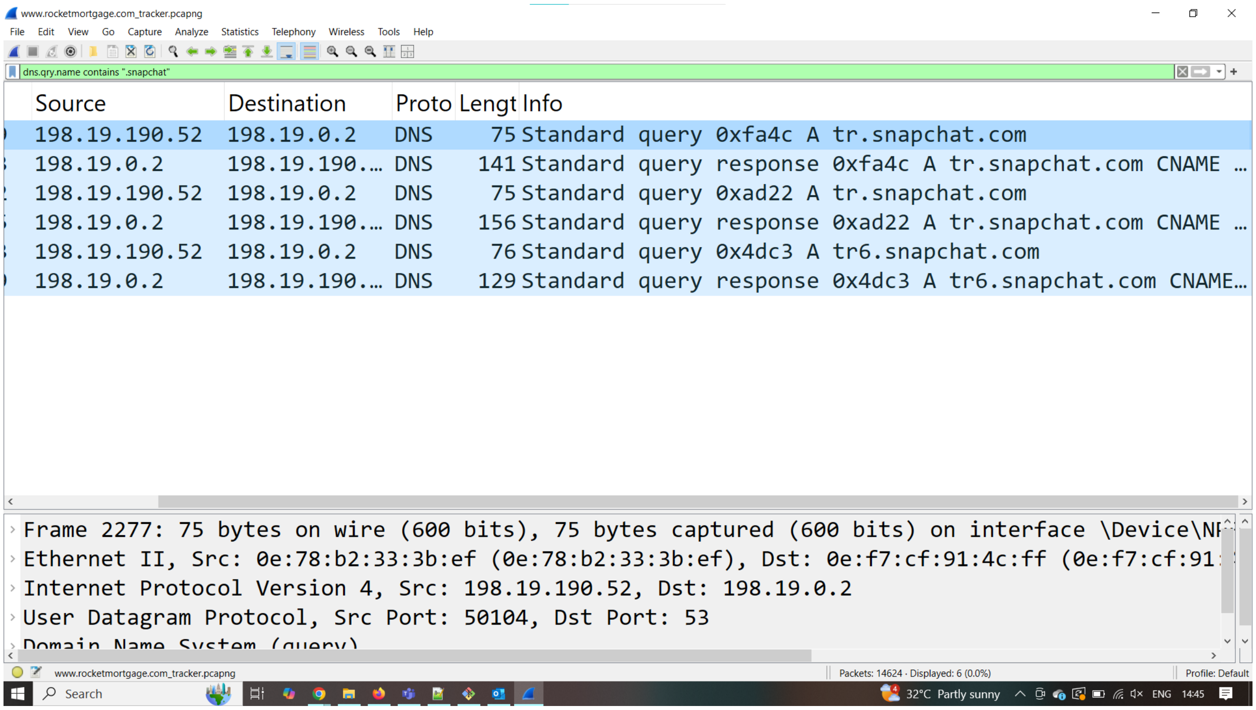
29 / 202 requests | 1.0 kB / 1,009 kB transferred | 0.5 kB / 2,794 kB resources

/ /

/ /

/ /

Figure 8



www.rocketmortgage.com_tracker.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
dns.qry.name contains ".snapchat"

Source          Destination     Proto Lengt Info
198.19.190.52   198.19.0.2      DNS      75 Standard query 0xfa4c A tr.snapchat.com
198.19.0.2      198.19.190.…    DNS     141 Standard query response 0xfa4c A tr.snapchat.com CNAME …
198.19.190.52   198.19.0.2      DNS      75 Standard query 0xad22 A tr.snapchat.com
198.19.0.2      198.19.190.…    DNS     156 Standard query response 0xad22 A tr.snapchat.com CNAME …
198.19.190.52   198.19.0.2      DNS      76 Standard query 0x4dc3 A tr6.snapchat.com
198.19.0.2      198.19.190.…    DNS     129 Standard query response 0x4dc3 A tr6.snapchat.com CNAME…

Frame 2277: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NF
Ethernet II, Src: 0e:78:b2:33:3b:ef (0e:78:b2:33:3b:ef), Dst: 0e:f7:cf:91:4c:ff (0e:f7:cf:91:
Internet Protocol Version 4, Src: 198.19.190.52, Dst: 198.19.0.2
User Datagram Protocol, Src Port: 50104, Dst Port: 53
Domain Name System (query)

www.rocketmortgage.com_tracker.pcapng    Packets: 14624 · Displayed: 6 (0.0%)    Profile: Default
```

97. The collection of Plaintiff's and Class Members' personally identifying and non-anonymized information through Defendant's installation and use of the Snapchat Tracker constitutes an invasion of privacy and violates CIPA. Cal. Penal Code § 638.51(a).

98. The Website transmits tracking signals to Snapchat immediately upon page load and continues to initiate communications with Snapchat's servers when a user navigates between pages. These transmissions allow Snapchat to persistently track user activity across multiple areas of the Website during a single session.

99. The Snapchat Tracker facilitates identity resolution by collecting browser metadata, device identifiers, and behavioral signals from users' sessions on the Website. These data points including IP addresses, user-agent strings, session timing, and specific pageview events are transmitted to Snapchat's servers immediately upon page load.

100. Defendant surreptitiously installed, executed, embedded, or injected the Snapchat Tracker by deploying Snapchat's JavaScript tracking code through dynamic

injection on the Website. When a user visits the Website, their browser executes the script, which transmits data about the user's interactions including the user's IP address, page URL, and other metadata to Snapchat's servers. This communication occurs silently and automatically, without any user action or awareness.

101. The Snapchat Tracker is at least a "process" because it is software that identifies consumers, gathers data, and correlates that data.

102. The Snapchat Tracker is at least a "device" because in order for software to work, it must be run on some kind of computing device. *See*, e.g., *James v. Walt Disney Co.* 2023 WL 7392285 at *13 (N.D. Cal. Nov. 8, 2023).

103. The Snapchat tracker functions as a pen register or trap and trace device because it is designed to capture and transmit addressing, signaling, and routing information associated with a user's interactions on a website, including such information as page URLs, video identifiers, device and browser metadata, IP address, click paths, scroll depth, and session timestamps. This data reveals the origin and destination of electronic communications, closely analogous to how a traditional pen register captures dialed numbers and a trap and trace device records incoming call data. By systematically logging which content the user accessed (i.e., the "addressed" destination), the technical attributes of the user's system (i.e., the "signaling"), and the communication route (i.e., IP routing and timestamps), the Snapchat tracker enables TikTok to identify patterns of communication behavior, monitor content consumption in real time, and attribute it to specific individuals or devices.

104. Defendant never obtained a court order permitting the installation of a pen register or trap and trace device or process and did not obtain Plaintiff's or the Class Members' express or implied consent to install the Snapchat Tracker on Plaintiff's and Class Members' browser or to collect or share data with Snapchat.

105. Consequently, the Defendant's secret installation of the Snapchat tracker violates CIPA regarding unauthorized use of a pen register and/or trap and trace device without prior consent or court order.

VI. CLASS ALLEGATIONS

106. Plaintiff brings this action individually and on behalf of all others similarly situated (the "Class" or "Class Members") defined as follows:

> All persons within California whose browser was subject to installation, execution, embedding, or injection of the Trackers by the Defendant's Website during the relevant statute of limitations period.

107. **NUMEROSITY:** Plaintiff does not know the number of Class Members but believes the number to be in the thousands, if not more. The exact identities of Class Members can be ascertained by the records maintained by Defendant.

108. **COMMONALITY:** Common questions of fact and law exist as to all Class Members and predominate over any questions affecting only individual members of the Class. Such common legal and factual questions, which do not vary between Class members, and which may be determined without reference to the individual circumstances of any Class Member, include but are not limited to the following:

- Whether Defendant installed, executed, embedded or injected the Trackers on the Website;
- Whether the Trackers are each a pen register and/or trap and trace device as defined by law;
- Whether Plaintiff and Class Members are subject to same tracking policies and practices;
- Whether Plaintiff and Class Members are entitled to statutory damages;
- Whether Class Members are entitled to injunctive relief;
- Whether Class Members are entitled to disgorgement of data unlawfully obtained;
- Whether the Defendant's conduct violates CIPA; and
- Whether the Defendant's conduct constitutes an unlawful, misleading, deceptive or fraudulent business practice.

109. **TYPICALITY:** As a person who visited Defendant's Website and whose outgoing electronic information was surreptitiously collected by the Trackers, Plaintiff is asserting claims that are typical of the Class Members. Plaintiff's experience with the Trackers is typical to Class Members.

110. **ADEQUACY:** Plaintiff will fairly and adequately protect the interests of the members of the Class. Plaintiff has retained attorneys experienced in class action litigation. All individuals with interests that are actually or potentially adverse to or in conflict with the Class or whose inclusion would otherwise be improper are excluded.

111. **SUPERIORITY:** A class action is superior to other available methods of adjudication because individual litigation of the claims of all Class Members is impracticable and inefficient. Even if every Class Member could afford individual litigation, the court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed.

VII. FIRST CAUSE OF ACTION

Violations of Cal. Penal Code § 638.51

By Plaintiff and the Class Members Against All Defendants

112. Plaintiff reasserts and incorporates by reference the allegations set forth in each preceding paragraph as though fully set forth herein.

113. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

114. Defendant uses a pen register device or process and/or a trap and trace device or process on its Website by deploying the Trackers because the Trackers are designed to capture the IP address, User Information and other information such as the phone number, email, routing, addressing and/or other signaling information of website visitors.

115. Defendant did not obtain consent from Plaintiff or any of the Class Members before using pen registers or trap and trace devices to locate or identify users of its Website and has thus violated CIPA. CIPA imposes civil liability and statutory

penalties for violations of § 638.51. Cal. Penal Code § 637.2; *Moody v. C2 Educational Systems, Inc.*, No. 2:24-cv-04249-RGK-SK, 2024 U.S. Dist. LEXIS 132614 (C.D. Cal. July 25, 2024).

VIII. <u>SECOND CAUSE OF ACTION</u>

Violations of Business & Professions Code § 17200

By Plaintiff and the Class Members Against All Defendants

116. Plaintiff realleges and incorporates by reference all preceding paragraphs of this Complaint as though fully set forth herein.

117. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

118. This cause of action is brought under California Business & Professions Code § 17200 et seq., which prohibits any unlawful, unfair, or fraudulent business act or practice.

119. Defendant has engaged in unlawful business practices by:

(a) Violating California Penal Code §§ 638.50–638.56, including the unauthorized collection of addressing, signaling, and routing information for user identification and tracking; and

(b) Violating California Civil Code § 1798.100, *et seq.*, including collecting, using, and/or selling Plaintiff's and Class Members' personal information and location data to Third Parties without providing sufficient notice. Privacy rights rooted in the CCPA are a protected interest enforceable under Business & Professions Code § 17200. *Briskin v. Shopify, Inc.*, 101 F.4th 706 (9th Cir. 2025) (en banc).

120. Defendant has engaged in unfair business practices by embedding the Trackers into the Website and enabling the real-time capture and transmission of Plaintiff's and Class Members' personal and behavioral information, such as IP address, browser details, visited URLs, referrer paths, timestamps, and interaction events, to the Third Parties.

121. The Defendant's practices are contrary to public policy supporting

consumer privacy and data autonomy, and the harm it causes to consumers, including loss of control over personal information and risk of profiling, outweighs any legitimate business justification.

122. Defendant has engaged in fraudulent business practices by failing to adequately disclose its data-sharing practices. On information and belief, Defendant omitted material facts from its privacy policy and/or site interface and failed to inform users that their activities would be tracked across the internet and linked to unique identifiers for advertising and profiling purposes. These omissions were likely to deceive a reasonable consumer and were intended to obscure the nature and extent of the surveillance.

123. As a direct and proximate result of Defendant's unlawful, unfair, and fraudulent conduct, Plaintiff and the Class Members have suffered injury in fact and loss of money or property, including the unauthorized exfiltration and commodification of valuable personal data. Plaintiff's and Class Members' data—used for targeted advertising, behavioral modeling, and enrichment by third parties—constitutes digital property with measurable economic value.

124. Plaintiff on behalf of herself and on behalf of the Class Members seeks injunctive relief to prevent Defendant from continuing its deceptive and unlawful data tracking practices and to require clear and conspicuous notice and opt-in consent for any behavioral tracking involving third-party tools. Plaintiff on behalf of herself and on behalf of the Class Members, also seeks restitution of the value derived from the unauthorized use of their personal information, attorneys' fees where permitted by law, and such other and further relief as the Court may deem just and proper.

IX. **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff prays for the following:

1. An order certifying the Class, naming Plaintiff as Class representative, and naming Plaintiff's attorneys as Class counsel;
2. An order declaring that Defendant's conduct violates CIPA and Business

& Professions Code § 17200;

3. An order of judgment in favor of Plaintiff and the Class against Defendant on the causes of action asserted herein;
4. An order enjoining Defendant's conduct as alleged herein;
5. Statutory damages pursuant to CIPA;
6. Prejudgment interest;
7. Reasonable attorney's fees and costs; and
8. All other relief that would be just and proper as a matter of law or equity.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all claims so permitted.

Dated: July 23, 2025 **NATHAN & ASSOCIATES, APC**

By: /s/ Reuben D. Nathan
Reuben D. Nathan, Esq.
Attorneys for Plaintiff